



StoneGate SG-200 Appliance Installation Guide

Copyright © 2001–2006 Stonesoft Corp. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from Stonesoft Corporation.

Stonesoft Corporation
Itälähdenkatu 22 A
FI-00210 Helsinki
Finland

Stonesoft Inc.
1050 Crown Pointe Parkway,
Suite 900
Atlanta, GA 30338 USA

Trademarks and Patents

The products described in this documentation are protected by U.S. Patents and European Patents: U.S. Patents no. 6,650,621, 6,856,621, 6,912,200, and 6,996,573; European patents no. 1065844, 1259028, 1289183, 1289202, 1326393, 1361724, and 1379037; and may be protected by other US patents, foreign patents, or pending applications.

Stonesoft, the Stonesoft logo, StoneBeat, FullCluster, ServerCluster, StoneGate, and WebCluster are trademarks or registered trademarks of Stonesoft Corporation in the United States and/or other countries. Multi-Link technology, Multi-Link VPN, and the StoneGate clustering technology as well as other technologies included in StoneGate are protected by patents or pending patent applications in the U.S. and other countries.

Sun, Sun Microsystems, Solaris, and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Windows and Microsoft are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds.

All other trademarks or registered trademarks are property of their respective owners.

Disclaimer

Although every precaution has been taken to prepare these materials, Stonesoft assumes no responsibility for errors, omissions, or resulting damages from the use of the information contained herein. All IP addresses in these materials were chosen at random and are used for illustrative purposes only. They are not intended to represent the IP addresses of any specific individual or organization.

THESE MATERIALS ARE PROVIDED "AS-IS." STONESOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO, THE INFORMATION CONTAINED HEREIN. IN ADDITION, STONESOFT MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT THE INFORMATION OR TECHNIQUES CONTAINED IN THESE MATERIALS. IN NO EVENT SHALL STONESOFT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING FROM THE USE OF THESE MATERIALS, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Introduction

Thank you for choosing Stonesoft's StoneGate™ appliance. This guide provides instructions for the initial hardware installation and the maintenance of the SG-200 appliances.

Contents

- [Getting Started](#), 4
- [Safety Precautions](#), 7
- [Front Panel](#), 9
- [Connecting the Cables](#), 10
- [Initial Configuration](#), 11

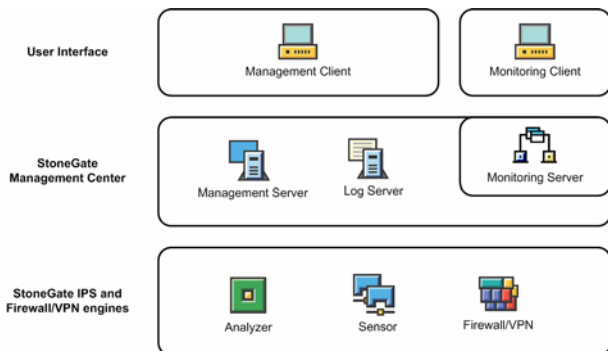


Caution – Never open the covers of the appliance! There are no user serviceable parts inside. Opening the covers may lead to serious injury and will void the warranty. Read the [Safety Precautions](#), on page 7 before you conduct any installation or maintenance operations on the appliance.

Getting Started

StoneGate System Components

Illustration 1 StoneGate Components



The illustration above shows all available StoneGate components. Out of these, you need the following components to have an operational Firewall/VPN system:

1. A **Management Server**, which stores the configuration of the system. In most environments, it is best to have just one common Management Server for all firewall and IPS engines.
2. At least one **Log Server** to handle and store logs and alerts (can be installed simultaneously on the same machine with the Management Server).
3. At least one **Management Client** that you use to connect to the Management Server to change settings and monitor the system.
4. The **Firewall Engines** that handle the actual traffic processing (in this case, the SG-200 appliance).
5. **Licenses** for each component except the Management Client(s).

The **Monitoring Server** and the **Monitoring Client** are optional components that are available on separate order.

StoneGate IPS engines can be added to the same system for unified management and incident handling.

The installation procedure is outlined on the next page. Only the hardware-related tasks that concern SG-200 appliances are covered in this booklet.

Installation Procedure

The appliance installation involves the following mandatory steps:

1. Configure the Firewall element in the Management Center (see the separate *StoneGate Installation Guide* or the online help of the Management Client).
2. Save the initial configuration to receive a one-time password for establishing trust between the appliance and the Management Server (see the separate *StoneGate Installation Guide*).
3. Connect the cables as instructed in this guide.
4. Perform the initial configuration and establish contact between the appliance and the Management Server (see *Initial Configuration*, on page 11).

Product Documentation

The following documentation covers the StoneGate Firewall/VPN products:

- The *Installation Guide* explains how to install the Management Center and configure your firewalls' basic settings.
- The *online help* system of the Management Client contains the step-by-step instructions for the daily configuration and management of your system.
- The *Administrator's Guide* contains the same information as the online help system, but in PDF form.
- The *Reference Guide* contains background and reference information that helps you to plan and understand your system.

Finding the Documentation

Press F1 while in any Management Client window to view the online help.

All PDF guides are available:

- On the Management Center CD-ROM (in the Documentation folder)
- At the Stonesoft Website at my.stonesoft.com/download/doc

The *Installation Guide* and *Reference Guide* are delivered as printed books if so requested in your order.

Install the free Adobe Reader program to view the PDF documents (available at www.adobe.com/reader/).

Safety Precautions

The following safety information and procedures must be followed whenever working with the StoneGate Appliance. However, please be advised that StoneGate Appliances are not end-user serviceable, and you must never open the appliance chassis for any reason. Doing so may lead to serious injury and will void any hardware warranty that may be associated with your appliance.

Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the appliance from damage:

- Be aware of the locations of the power on/off switch as well as the room's emergency power-off switch, disconnection switch, or electrical outlet. If an electrical accident occurs, you can then quickly cut power to the system.
- Do not work alone when working with high voltage components.
- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards they come into contact with.
- Do not use mats designed to decrease electrostatic discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- The power supply cord must include a grounding plug and must be plugged into a grounded electrical outlet.



Caution – Never open the appliance chassis! There are no user serviceable parts inside. Opening the chassis may lead to serious injury and will void the warranty.

General Safety Precautions

Follow these rules to ensure general safety:

- Keep the area around the appliance clean and free of clutter.
- We recommend using a regulating uninterruptible power supply (UPS) to protect the appliance from power surges, voltage spikes and to keep your system operating in case of a power failure.

ESD Precautions

Electrostatic discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards. Use a grounded wrist strap designed to prevent static discharge.

Note – Use a UPS (Uninterruptible Power Supply) in critical environments with your StoneGate appliance. If after a brief power outage your StoneGate appliance only partially starts up (for example, the power light is on, but the NIC LEDs are off and the appliance does not connect) turn the appliance off for five seconds and then back on.

Operating Precautions

Care must be taken to assure that the chassis cover is in place when the appliance is operating to ensure proper cooling. Out of warranty damage to the appliance system can occur if this practice is not strictly followed.

Lithium Battery Precautions

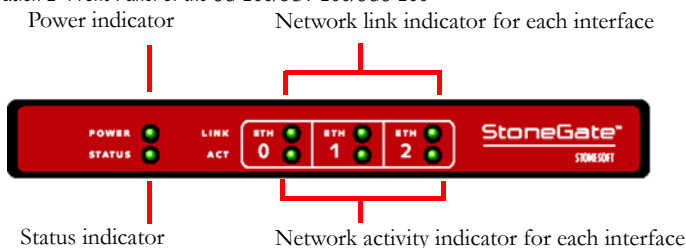


Do not change the battery; the battery must be replaced by authorized service personnel only. Danger of explosion if battery is incorrectly replaced. Replacement battery must be same or equivalent type recommended by the manufacturer. Used batteries must be discarded according to the manufacturer's instructions. Short-circuiting the battery may heat the battery and cause severe injuries.

Front Panel

Illustration 2 shows the front panel of the SG-200/SGV-200/SGS-200.

Illustration 2 Front Panel of the SG-200/SGV-200/SGS-200



Parts Included

If your box has missing or damaged parts, inform Stonesoft as soon as possible. Refer to the warranty for more information.

The appliance package should include the following items:

- StoneGate appliance
- This *StoneGate Appliance Installation Guide*
- AC power cord
- Serial (null modem) cable.

Connecting the Cables

Illustration 3 shows the back panel of the SG-200/SGV-200/SGS-200.

Illustration 3 Back Panel of the SG-200/SGV-200/SGS-200



Connect the cables as follows:

1. Connect the network cables to the LAN ports.
2. Connect the supplied serial cable to the serial port and to the serial port of a computer that you will use to configure the appliance.
3. Connect the power cable to the appliance, but do not connect the power cable to a power source yet.

Note – When the appliance is powered and you need to unplug it, always wait at least five (5) seconds before plugging in the appliance again. Otherwise, the appliance may not have time to clear properly and fails to start.

Initial Configuration

Your StoneGate appliance comes pre-loaded with StoneGate engine software. However, before a security policy can be loaded on the appliance, you must configure the engine software. To successfully complete the configuration:

- The Firewall element must be defined in the Management Center
- You must have created a one-time password for this engine. See the *StoneGate Installation Guide* for details.

Note – The appliance must contact the Management Server before it can be operational.

▼ To start the appliance

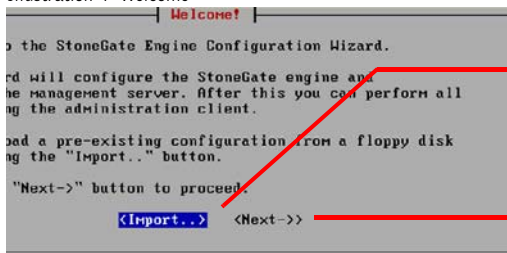
1. Make sure you have a physical connection to the appliance using a monitor and keyboard or a serial cable (see [Connecting the Cables](#), on page 10).
 - When using a serial line connection, use the terminal settings 9600bps, 8 databits, 1 stopbit, no parity.
2. Turn on the power using the power on/off button. The engine bootup process is shown in the console and, after some time, the engine configuration wizard starts.

You can return to the engine configuration wizard at any time using the sg-reconfigure command on the engine command line.

Configuring the Firewall

▼ To select the configuration

Illustration 4 Welcome



To import a saved configuration, highlight **Import** using the arrow keys and press ENTER.

To skip the import, highlight **Next** and press ENTER.

▼ To set the keyboard layout

Illustration 5 Configure OS Settings

Highlight the entry field for **Keyboard Layout** using the arrow keys and press ENTER. The Select Keyboard Layout dialog opens.



Illustration 6 Select Keyboard Layout

Highlight the correct layout and press ENTER.

Tip: Type in the first letter to move forward more quickly.



Note – If the desired keyboard layout is not available, use the best-matching available layout, or select US_English.

▼ To set the engine's timezone

Illustration 7 Configure OS Settings

1. Highlight the entry field for **Local Timezone** using the arrow keys and press ENTER.
2. Select the correct Keyboard Layout in the dialog that opens.



Note – The timezone setting affects only the way the time is displayed on the engine command line. The actual operation always uses UTC time.

Note – The appliance's clock is automatically synchronized with the Management Server clock.

▼ To set the rest of the OS settings

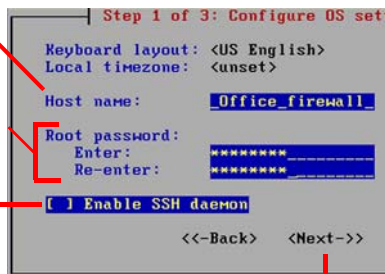
Illustration 8 Configure OS Settings

1. Type in the name of the firewall.

2. Type in the password for the user **root**. This is the only account for engine command line access.

3. Highlight **Enable SSH Daemon** and press the spacebar on your keyboard to select the option and allow remote access to engine command line using SSH.

4. Highlight **Next** and press ENTER. The Configure Network Interfaces window is displayed.



Configuring the Network Interfaces

The configuration utility can automatically detect which network cards are in use. You can also add interfaces manually, if necessary.

▼ To add the network interfaces

Illustration 9 Configure Network Interfaces



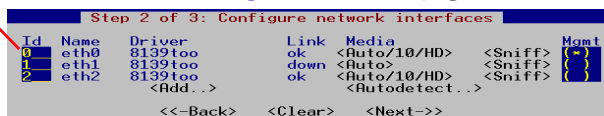
Highlight **Autodetect** and press ENTER.

Check that the automatically detected drivers are correct and that all interfaces have been detected. To add interfaces manually, click **Add** and select a device driver.

▼ To map the physical interfaces to interface IDs

Illustration 10 Assigning Network Interfaces

1. Type in the IDs to define how physical interfaces are mapped to the Interface IDs you defined in the Firewall element. Ethernet ports are detailed in [Illustration 3](#) in [Connecting the Cables](#), on page 10.



Id	Name	Driver	Link	Media		Mgmt
0	eth0	8139too	ok	<Auto/10/HD>	<Sniff>	{ }
1	eth1	8139too	down	<Auto>	<Sniff>	{ }
2	eth2	8139too	ok	<Auto/10/HD>	<Sniff>	{ }
		<Add...>		<Autodetect...>		
<<Back> <Clear> <Next-->						

2. Highlight and press ENTER to match the speed/duplex settings to those used in each network.

3. Highlight the **Mgmt** column and press the spacebar on your keyboard to select the correct interface for contact with the Management Server.

Note – The Management interface must be the same that you configured as the Primary Control Interface for the corresponding Firewall element in the Management Center.

Highlight **Next** and press ENTER to continue.

Contacting the Management Server

The Prepare for Management Contact window opens. If the initial configuration was imported, most of this information is filled in.

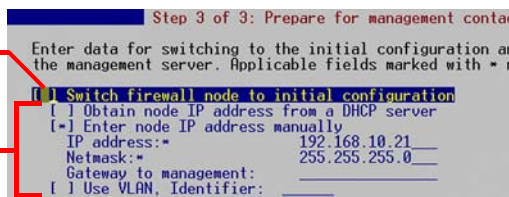
This task has two parts. First, you activate an initial configuration on the firewall.

- The initial configuration contains the information that the engine needs to connect to the Management Server for the first time.
- The initial configuration is replaced with a working configuration when you install a Firewall Policy from the Management Server on this engine using the Management Client.

▼ To activate the initial configuration

Illustration 11 Prepare for Management Contact - Upper Part

1. Highlight **Switch Firewall Node to Initial Configuration** and press spacebar to activate.



2. Fill in according to your environment. The information must match to what you defined for the Firewall element (Primary Control IP Address). If the engine and the Management Server are on the same network, you can leave the **Gateway to management** field empty.

The initial configuration contains a simple firewall policy that allows only administration-related connections and blocks everything else.

▼ To fill in the Management Server information

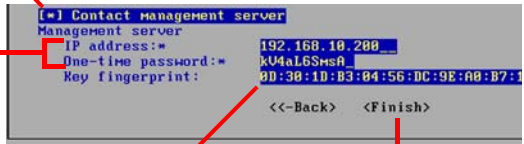
In the second part of the configuration, you define the information needed for establishing a trust relationship between the engine and the Management Server.

If you do not have a one-time password for this firewall, see the *Installation Guide* for instructions on how to save an initial configuration.

Illustration 12 Prepare for Management Contact - Lower Part

1. Highlight **Contact Management Server** and press spacebar to activate.

2. Fill in the Management Server IP address and the one-time password that was created for this engine when you saved the initial configuration.



3. (Optional) Fill in the Key fingerprint (also shown when you saved the initial configuration). Filling it in increases the security of the communications.

4. Highlight **Finish** and press ENTER.

Note – Once initial contact has been made, the engine receives a certificate from the Management Center for identification. If the certificate is deleted or expires, you must repeat the initial contact using a new one-time password.

The engine now tries to make initial Management Server contact.

- If you see a “connection refused” error message, ensure that the one-time password is correct and the Management Server IP address is reachable from the node. Save a new initial configuration if unsure about the password.
- If the engine is unable to contact the Management Server, make sure there are no networking problems, that all information defined in the Firewall element corresponds to what you entered in the Configuration wizard and, if NAT is in use, that you have configured contact addresses for NAT as explained in the *Installation Guide*.

After Successful Management Server Contact

After you see a notification that Management Server contact has succeeded, the firewall engine installation is complete and the firewall is ready to receive a policy. In a while, the firewall’s status changes in the Management Client from **Unknown** to **No Policy Installed**, and the

connection state is **Connected** indicating that the Management Server can connect to the node.

The next step is creating a security policy and installing it on the engine. Please see the *Installation Guide* for basic instructions or the online help system of the Management Client for detailed instructions.



Caution – When using the command prompt, use the `reboot` command to reboot and `halt` command to shut down the node. Do not use the `init` command. You can also reboot the node using the Management Client.
